Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Previously Presented) A data transfer method performed at a proxy server, the method comprising:

intercepting a data request from a client computer that is directed to a target server;

encrypting profile information;

appending the encrypted profile information to the data request as originally intercepted to create an augmented data request; and

sending the augmented data request to the target server.

2. (Original) The method of claim 1 further comprising:

receiving a reference token from the target server;

receiving a second data request from the client computer that is directed to the target server;

augmenting the second data request by adding the reference token to the second data request; and

sending the augmented second data request to the target server.

3. (Original) The method of claim 2 wherein the reference token comprises a reference to the profile information sent to the target server.

4. (Original) The method of claim 1 further comprising retrieving the profile information from a database based on an identity of a user.

5. (Original) The method of claim 4 further comprising using the Internet Engineering Task Force IDENT protocol to determine the identity of the user.

6. (Original) The method of claim 1 wherein encrypting profile information comprises determining a session key and using the session key as an encryption key.

7. (Original) The method of claim 6 further comprising encrypting the session key, and wherein augmenting the data request further comprises adding the encrypted session key to the data request.

8. (Original) The method of claim 7 wherein using the session key to encrypt the profile information comprises using the session key as a symmetric encryption algorithm encryption key, and wherein encrypting the session key comprises encrypting using a public key encryption algorithm and a public key associated with the target server.

9. (Original) The method of claim 8 further comprising obtaining the public key from the target server.

10. (Original) The method of claim 9 wherein obtaining the public key from the target server comprises sending a request to the target server to retrieve the public key.

11. (Original) The method of claim 1 wherein the data request comprises a hypertext transfer protocol (HTTP) request comprising a HTTP field, the target server comprises a HTTP server, and the client computer comprises a web browser application.

12. (Original) The method of claim 1 wherein the profile information comprises information associated with the client computer.

13. (Previously Presented) A data transfer method performed at an information server, the method comprising:

receiving an augmented data request, wherein the augmented data request includes encrypted user profile information appended to a data request as originally intercepted by a proxy server;

extracting the encrypted user profile information added to the data request by the proxy server;

using the extracted profile information to generate a response; and

sending the response to the proxy server.

14. (Previously Presented) The method of claim 13 wherein using the extracted user profile information to generate a response comprises providing the extracted user profile information to a web application and generating the response by processing the web application.

15. (Previously Presented) The method of claim 14 wherein providing the extracted user profile information comprises setting HTTP environment variables at a web server and wherein the web application comprises a common gateway interface script.

16. (Previously Presented) The method of claim 13 further comprising storing the extracted user profile information at the information server and associating a reference token with the stored user profile information, and wherein the response further comprises the reference token.

17. (Previously Presented) The method of claim 16 further comprising:

receiving from the proxy server a second data request comprising the reference token;

extracting the reference token from the second data request;

accessing the stored user profile information based on the reference token; and

using the stored user profile information to generate a response to the second data request.

18. (Previously Presented) The method of claim 13 wherein extracting the user profile information comprises decrypting the user profile information.

19. (Previously Presented) The method of claim 18 wherein the data request further comprises a session key added to the data request by the proxy server and wherein decrypting the user profile information comprises using the session key to decrypt the user profile information.

20. (Original) The method of claim 19 further comprising decrypting the session keys.

21. (Original) The method of claim 20 wherein decrypting the session key comprises decrypting using a public key algorithm and a private key of the information server, and wherein decrypting using the session key comprises decrypting using a symmetric decryption algorithm.

22. (Previously Presented) A computer program residing on a computer-readable medium, comprising instructions for causing a computer to:

intercept a data request from a client computer that is directed to a target server;

encrypt profile information;

append the encrypted profile information to the data request as originally intercepted to create an augmented data request; and

send the augmented data request to the target server.

23. (Original) The program residing on the computer-readable medium of claim 22 further comprising instruction for causing a computer to:

receive a reference token from the target server;

receive a second data request from the client computer that is directed to the target server;

augment the second data request by adding the reference token to the second data request; and

send the augmented second data request to the target server.

24. (Original) The program residing on the computer-readable medium of claim 22 wherein:

the instructions for causing the computer to encrypt profile information comprise instructions to encrypt the profile information using a session key and a symmetric encryption algorithm;

the program further comprises instructions to encrypt the session key using a public key encryption algorithm; and

the instructions to augment the data request further comprise instructions to add the encrypted session key to the data request.

25. (Previously Presented) A computer program residing on a computer-readable medium, comprising instructions for causing a computer to:

receive a data request comprising encrypted profile information appended to the data request as originally intercepted by a proxy server;

extract the profile information added by the proxy server;

use the extracted profile information to generate a response; and

send the response to the proxy server.

26. (Original) The program residing on the computer-readable medium of claim 25 further comprising:

instructions for causing a computer to:

store the extracted profile information;

associate a reference token with the stored profile information;

include the reference token in the response to the proxy server;

receive from the proxy server a second data request comprising the reference token;

extract the reference token;

access the stored profile information based on the presence of the reference token in the

second data request; and

use the accessed profile information to generate a response to the second data request.

27. (Original) The program residing on the computer-readable medium of claim 25

wherein:

the data request further comprises encrypted session key information;

the program further comprises instructions for causing the computer to decrypt the

session key information; and

the instructions to extract the profile information comprises instructions for causing the

computer to decrypt the profile information using the decrypted session key.

28. (Previously Presented) A proxy server comprising:

a database comprising records storing user profile information;

a network interface operatively coupled to a network to exchange data with a client

computer and with a target server; and

a processor operatively coupled to the network interface, the database, and a memory

comprising executable instructions for causing the processor to intercept a data

request that is directed to a target server, retrieve a record from the database, encrypt profile

information in the record, append the encrypted profile information to the data request as

originally intercepted to create an augmented data request, and send the augmented data request

to the target server

29. (Original) The proxy server of claim 28 wherein the memory further comprises

instructions for causing the processor to receive a reference token from the target server, receive

a second data request from the client computer that is directed to the target server, augment the

second data request by adding the reference token to the second data request, and send the

augmented second data request to the target server.

Applicant : Larry T. HARADA et al.   Attorney's Docket No.: 06975-041001 / Security 01
Serial No. : 09/323,415
Filed   : June 1, 1999
Page   : 8 of 15

30. (Original) The proxy server of claim 28 wherein:

the instructions for causing the computer to encrypt the profile information comprise instructions to encrypt the profile information using a session key and a symmetric encryption algorithm;

the memory further comprises instructions to encrypt the session key using a public key encryption algorithm; and

the instructions to augment the data request further comprise instructions to add the encrypted session key to the data request.

31. (Previously Presented) An information server comprising:

a network interface operatively coupling the information server to a proxy server; and

a processor operatively coupled to the network interface and to a memory comprising executable instructions for causing the processor to receive an augmented data request from the proxy server, wherein the augmented data request includes encrypted user profile information appended to a data request as originally intercepted by the proxy server, decrypt the encrypted user profile information; and use the decrypted user profile information to generate a response to the augmented data request.

32. (Previously Presented) The server of claim 31 wherein the memory further comprise instructions to decrypt an encrypted session key added to the data request by the proxy server, and the instructions to decrypt user profile information further comprise instructions to decrypt the user profile information using the decrypted session key.

33. (Currently Amended) A method performed at a proxy server, the method comprising:

receiving intercepting a request from a client;

determining destination information associated with the request;

determining that a target server associated with the destination information should receive user profile information;

encrypting user profile information;

appending the encrypted profile information to the data request as originally intercepted to create an augmented data request; and

sending the augmented request to the target server.

34. (Previously Presented) The method of claim 33 further comprising:

determining a valid public key for the target server;

encrypting a session key using the public key; and

augmenting the request by adding the encrypted session key

35. (Previously Presented) The method of claim 34 further comprising:

determining a valid public key for the target server;

encrypting a session key information using the public key;

encrypting the user profile information using the encrypted session key; and

augmenting the request by adding the public key, encrypted session key, and encrypted user profile information to the request.

36. (Currently Amended) The method of claim 33 wherein determining that the target server should receive user profile information includes querying a database associated with the proxy server to determine if the target server should receive user profile information.

37. (Previously Presented) The method of claim 33 further comprising receiving a token from the target server and providing the token with other requests associated with the user profile that are directed to the target server.

38. (Currently Amended) A system comprising:

a proxy server to:

~~receive~~-intercept a request from a client;

determine destination information associated with the request;

determine that a target server associated with the destination information should receive user profile information;

encrypting user profile information;

appending the encrypted profile information to the data request as originally intercepted to create an augmented data request; and

send the augmented request to the target server.

39. (Previously Presented) The system of claim 38 wherein the proxy server is configured to:

determine a valid public key for the target server;

encrypt a session key information using the public key; and

augment the request by adding the encrypted session key.

40. (Currently Amended) The system of claim 38 wherein the proxy server is configured to:

determine a valid public key for the target server;

encrypt a session key information using the public key;

encrypt the user profile information using the encrypted session key; and

augment the request by adding the public key, encrypted session key, and encrypted user profile information to the request.

41. (Currently Amended) The system of claim 40 wherein the proxy server is configured to:

Applicant : Larry T. HARADA et al.   Attorney's Docket No.: 06975-041001 / Security 01
Serial No. : 09/323,415
Filed   : June 1, 1999
Page   : 11 of 15

determine the target server should receive user profile information ~~includes~~ by querying a database associated with the proxy server to determine if the target server should receive user profile information.

42. (Previously Presented) The system of claim 41 further comprising a target server wherein the target server is configured to:

    store the user profile information;

    send a token to the proxy server;

    receive the token with a subsequent request; and

    access the stored user profile information based on the token.

43. (Previously Presented) The method of claim 1 wherein the encrypted profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

44. (Previously Presented) The method of claim 13 wherein the encrypted user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

45. (Previously Presented) The program of claim 22 wherein the encrypted profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

46. (Previously Presented) The program of claim 25 wherein the encrypted profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

47. (Previously Presented) The proxy server of claim 28 wherein the encrypted profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

48. (Previously Presented) The information server of claim 31 wherein the encrypted user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

49. (Previously Presented) The method of claim 33 wherein the encrypted user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

50. (Previously Presented) The system of claim 38 wherein the encrypted user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.